UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/809,316	03/24/2004	David M. Durham	42P19298	6497

45209 7590 02/02/2009

INTEL/BSTZ
BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
SHIU, HO T	

ART UNIT	PAPER NUMBER
2457	

MAIL DATE	DELIVERY MODE
02/02/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/809,316	DURHAM ET AL.	
	Examiner	Art Unit	
	HO SHIU	2457	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 November 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10,12-29,31-48,50-67 and 69-76* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10, 12-29, 31-48, 50-67, and 69-76* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *10 November 2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-10, 12-29, 31-48, 50-67, and 69-76 are pending in this application. Claims 1, 20, 39, and 58 have been amended by amendment filed by Applicant on 11/10/2008.

Claim Objections

2. Claims 1 and 58 recites the limitation "embedded controller" and "embedded controller agent". The examiner notes that in similar claims, 20 and 39, there is only an embedded hardware controller agent. The examiner believes that the applicant has simply missed changing all embedded controller or variations there of to "embedded hardware controller agent". Appropriate correction is required

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. **Claims 1-10, 12-16, 18-29, 31-35, 37-48, 50-54, 56-67, 69-73, and 75-76 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gibbons et al. (US Patent # 6,243,809 B1, hereinafter Gibbons) in view of Rakavy et al. (US Patent #**

5,978,912 B2, hereinafter Rakavy) and in further view of Falik et al. (US Patent # 7,318,173 B1, hereinafter Falik) and in further view of Herzi (US Patent # 6,484,262, hereinafter Herzi) . Gibbons and Rakavy are cited in the Information Disclosure Statement filed by applicant on 05/09/2006.

5. With respect to claim 1, Gibbons discloses an apparatus comprising: an embedded firmware agent (fig. 6, col. 9, lines 34-37) having instructions that cause the embedded firmware agent to selectively operate in a management mode (col. 9, lines 37-43) during which a host operating system relinquishes control of a host system in which the embedded firmware agent resides (col. 2, lines 14-30); and a bi-directional agent bus coupled between the embedded firmware agent and the embedded controller agent to transmit messages between the embedded firmware agent and the embedded controller agent (fig. 6, col. 9, lines 34-37, fig. 7, col. 9, lines 44-52, fig. 2, col. 9, lines 36-52, in the specification [0019] a bi-directional agent bus can be any bi-directional communication mechanism. The embedded firmware agent of Gibbons (fig. 6, col. 9, lines 34-37) and the embedded controller agent (fig. 7, col. 9, lines 44-52) communicate via memory locations (fig. 2 (34), col. 9, lines 36-52) which is considered a bi-directional communication mechanism).

Gibbons does not clearly disclose the embedded hardware controller agent coupled within the host system having memory to store instructions that cause the embedded controller to operate independently of the host operating system and selectively invokes the management mode, the embedded controller agent having a

network interface to allow the embedded controller agent to communicate over a network independently of the host operating system, a physical bi-directional agent bus coupled between the embedded firmware agent and the embedded controller agent to transmit messages between the embedded firmware agent and the embedded controller agent; and a trusted module couple with the embedded hardware controller agent and the embedded firmware agent to provide mutual authentication with a server prior to the embedded firmware agent transferring control to the host operating system.

In the same field of endeavor, Rakavy discloses the embedded controller agent having a network interface to allow the embedded controller agent to communicate over a network independently of the host operating system (col. 1, lines 7-14, col. 4, lines 4-32).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Gibbons with the teachings of Rakavy in order to enhance a computer's BIOS to accommodate remote access and maintenance without the aid of the operating system executing on the computer.

However, Gibbons and Rakavy does not clearly disclose the embedded hardware controller agent coupled within the host system having memory to store instructions that cause the embedded controller to operate independently of the host operating system and selectively invokes the management mode, the embedded controller agent having a network interface to allow the embedded controller agent to communicate over a network independently of the host operating system, a physical bi-directional agent bus coupled between the embedded firmware agent and the

embedded controller agent to transmit messages between the embedded firmware agent and the embedded controller agent; and a trusted module couple with the embedded hardware controller agent and the embedded firmware agent to provide mutual authentication with a server prior to the embedded firmware agent transferring control to the host operating system.

In the same field of endeavor, Falik discloses the embedded hardware controller agent coupled within the host system having memory to store instructions that cause the embedded controller to operate independently of the host operating system and selectively invokes the management mode (fig. 4, col. 4 lines 1-15, if the CPU is not functioning, but the embedded controller is still able to switch to the other BIOS, this means that the embedded controller works independently of the host operating system, since SMBus is a physical connection, according to fig. 4, the SMBus connects to the embedded controller and the BIOS in which by inherent indicates that the embedded controller is a physical hardware), the embedded controller agent having a network interface to allow the embedded controller agent to communicate over a network independently of the host operating system (fig. 1, col. 5, lines 44-54), a physical bi-directional agent bus coupled between the embedded firmware agent and the embedded controller agent to transmit messages between the embedded firmware agent and the embedded controller agent (Fig. 4, col. 4, lines 25-45, col. 5, lines 6-26, SMBus is a physical bi-directional bus).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Gibbons and Rakavy with the teachings of Falik in order to remotely select a BIOS even if the CPU is not functioning.

However, Gibbons, Rakavy, and Falik do not clearly disclose a trusted module couple with the embedded hardware controller agent and the embedded firmware agent to provide mutual authentication with a server prior to the embedded firmware agent transferring control to the host operating system.

In the same field of endeavor, Herzi discloses a trusted module couple with the embedded hardware controller agent and the embedded firmware agent to provide mutual authentication with a server prior to the embedded firmware agent transferring control to the host operating system (col. 2, lines 45-64, col. 3, lines 18-34).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Gibbons, Rakavy, and Falik with the teachings of Herzi in order to provide an improved level of security and an improved security measure against undesired theft of a computer system.

6. With respect to claim 20, Gibbons discloses, a method comprising: invoking a management mode (col. 9, lines 45-52) in a host system in which a host operating system temporarily relinquishes control of the host system (col. 2, lines 25-33), and servicing requests from the embedded controller agent during the management mode with an embedded firmware agent by communicating with the embedded controller agent over a bidirectional agent bus (fig. 6, col. 9, lines 34-37, fig. 7, col. 9, lines 44-52,

fig. 2, col. 9, lines 36-52, in the specification [0019] a bi-directional agent bus can be any bi-directional communication mechanism. The embedded firmware agent of Gibbons (fig. 6, col. 9, lines 34-37) and the embedded controller agent (fig. 7, col. 9, lines 44-52) communicate via memory locations (fig. 2 (34), col. 9, lines 36-52) which is considered a bi-directional communication mechanism).

Gibbons does not clearly disclose with an embedded controller agent having a network connection that operates independently of the host operating system, an embedded firmware agent coupled within a host system having memory to store instructions, an embedded controller agent coupled within the host system having memory to store instructions that cause the embedded controller to operate.

In the same field of endeavor, Rakavy discloses an embedded controller agent having a network connection that operates independently of the host operating system (col. 1, lines 7-14).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Gibbons with the teachings of Rakavy in order to enhance a computer's BIOS to accommodate remote access and maintenance without the aid of the operating system executing on the computer.

However, Gibbons and Rakavy does not clearly disclose an embedded firmware agent coupled within a host system having memory to store instructions, an embedded controller agent coupled within the host system having memory to store instructions that cause the embedded controller to operate.

In the same field of endeavor, Falik discloses an embedded firmware agent coupled within a host system having memory to store instructions (col. 4, lines 50-62), an embedded controller agent coupled within the host system having memory to store instructions that cause the embedded controller to operate (col. 4, lines 65-6, col. 5, lines 1-10).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Gibbons and Rakavy with the teachings of Falik in order to remotely select a BIOS even if the CPU is not functioning.

However, Gibbons, Rakavy, and Falik do not clearly disclose a trusted module couple with the embedded hardware controller agent and the embedded firmware agent to provide mutual authentication with a server prior to the embedded firmware agent transferring control to the host operating system.

In the same field of endeavor, Herzi discloses a trusted module couple with the embedded hardware controller agent and the embedded firmware agent to provide mutual authentication with a server prior to the embedded firmware agent transferring control to the host operating system (col. 2, lines 45-64, col. 3, lines 18-34). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Gibbons, Rakavy, and Falik with the teachings of Herzi in order to provide an improved level of security and an improved security measure against undesired theft of a computer system.

The examiner notes that claim 20 is similar of claim 1, therefore is rejected for all the same reasons as claim 1 above.

7. With respect to claim 39, Gibbons discloses an article comprising a computer-readable medium having stored thereon instructions that, when executed, cause one or more processing elements to: invoke a management mode (col. 9, lines 45-52) in a host system in which a host operating system temporarily relinquishes control of the host system (col. 2, lines 25-33); and service requests from the embedded controller agent during the management mode with an embedded firmware agent by communicating with the embedded controller agent over a bi-directional agent bus (fig. 6, col. 9, lines 34-37, fig. 7, col. 9, lines 44-52, fig. 2, col. 9, lines 36-52, in the specification [0019] a bi-directional agent bus can be any bi-directional communication mechanism. The embedded firmware agent of Gibbons (fig. 6, col. 9, lines 34-37) and the embedded controller agent (fig. 7, col. 9, lines 44-52) communicate via memory locations (fig. 2 (34), col. 9, lines 36-52) which is considered a bi-directional communication mechanism).

Gibbons does not clearly disclose an embedded controller agent having a network connection that operates independently of the host operating system, an embedded firmware agent coupled within a host system having memory to store instructions, an embedded controller agent coupled within the host system having memory to store instructions that cause the embedded controller to operate.

In the same field of endeavor, Rakavy discloses an embedded controller agent having a network connection that operates independently of the host operating system (col. 1, lines 7-14).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Gibbons with the teachings of Rakavy in order to enhance a computer's BIOS to accommodate remote access and maintenance without the aid of the operating system executing on the computer.

However, Gibbons and Rakavy does not clearly disclose an embedded firmware agent coupled within a host system having memory to store instructions, an embedded controller agent coupled within the host system having memory to store instructions that cause the embedded controller to operate.

In the same field of endeavor, Falik discloses an embedded firmware agent coupled within a host system having memory to store instructions (col. 4, lines 50-62), an embedded controller agent coupled within the host system having memory to store instructions that cause the embedded controller to operate (col. 4, lines 65-6, col. 5, lines 1-10).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Gibbons and Rakavy with the teachings of Falik in order to remotely select a BIOS even if the CPU is not functioning.

However, Gibbons, Rakavy, and Falik do not clearly disclose a trusted module couple with the embedded hardware controller agent and the embedded firmware agent

to provide mutual authentication with a server prior to the embedded firmware agent transferring control to the host operating system.

In the same field of endeavor, Herzi discloses a trusted module couple with the embedded hardware controller agent and the embedded firmware agent to provide mutual authentication with a server prior to the embedded firmware agent transferring control to the host operating system (col. 2, lines 45-64, col. 3, lines 18-34). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Gibbons, Rakavy, and Falik with the teachings of Herzi in order to provide an improved level of security and an improved security measure against undesired theft of a computer system.

The examiner notes that claim 20 is similar of claim 1, therefore is rejected for all the same reasons as claim 1 above.

8. With respect to claim 58, Gibbons discloses a system comprising: a bus (col. 3, lines 47-50); a digital signal processor coupled with the bus (col. 4, lines 14-25, fig. 6, col. 9, lines 34-37); an embedded firmware agent coupled with the bus having instructions that cause the embedded firmware agent to selectively operate in a management mode (col. 9, lines 37-43) during which a host operating system relinquishes control of a host system in which the embedded firmware agent resides (col. 2, lines 25-33); an embedded controller agent (fig. 7, col. 9, lines 44-52) that operates independently of the host operating system (col. 2, lines 14-30) and selectively invokes the management mode (fig. 7, col. 9, lines 44-52); and a bi-directional agent

bus coupled between the embedded firmware agent and the embedded controller agent to transmit messages between the embedded firmware agent and the embedded controller agent (fig. 6, col. 9, lines 34-37, fig. 7, col. 9, lines 44-52, fig. 2, col. 9, lines 36-52, in the specification [0019] a bi-directional agent bus can be any bi-directional communication mechanism. The embedded firmware agent of Gibbons (fig. 6, col. 9, lines 34-37) and the embedded controller agent (fig. 7, col. 9, lines 44-52) communicate via memory locations (fig. 2 (34), col. 9, lines 36-52) which is considered a bi-directional communication mechanism).

Gibbons does not clearly disclose the embedded controller agent having a network interface to allow the embedded controller agent to communicate over a network independently of the host operating system, an embedded firmware agent coupled within a host system having memory to store instructions, an embedded controller agent coupled within the host system having memory to store instructions that cause the embedded controller to operate, and a physical bi-directional agent bus coupled between the embedded firmware agent and the embedded controller agent..

In the same field of endeavor, Rakavy discloses the embedded controller agent having a network interface to allow the embedded controller agent to communicate over a network independently of the host operating system (col. 1, lines 7-14).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Gibbons with the teachings of Rakavy in order to enhance a computer's BIOS to accommodate remote access and maintenance without the aid of the operating system executing on the computer.

However, Gibbons and Rakavy does not clearly disclose an embedded firmware agent coupled within a host system having memory to store instructions, an embedded controller agent coupled within the host system having memory to store instructions that cause the embedded controller to operate, and a physical bi-directional agent bus coupled between the embedded firmware agent and the embedded controller agent.

In the same field of endeavor, Falik discloses an embedded firmware agent coupled within a host system having memory to store instructions (col. 4, lines 50-62), an embedded controller agent coupled within the host system having memory to store instructions that cause the embedded controller to operate (col. 4, lines 65-6, col. 5, lines 1-10), and a physical bi-directional agent bus coupled between the embedded firmware agent and the embedded controller agent (Fig. 4, col. 4, lines 25-45, col. 5, lines 6-26, SMBus is a physical bi-directional bus).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Gibbons and Rakavy with the teachings of Falik in order to remotely select a BIOS even if the CPU is not functioning.

However, Gibbons, Rakavy, and Falik do not clearly disclose a trusted module couple with the embedded hardware controller agent and the embedded firmware agent to provide mutual authentication with a server prior to the embedded firmware agent transferring control to the host operating system.

In the same field of endeavor, Herzi discloses a trusted module couple with the embedded hardware controller agent and the embedded firmware agent to provide

mutual authentication with a server prior to the embedded firmware agent transferring control to the host operating system (col. 2, lines 45-64, col. 3, lines 18-34). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Gibbons, Rakavy, and Falik with the teachings of Herzi in order to provide an improved level of security and an improved security measure against undesired theft of a computer system.

The examiner notes that claim 20 is similar of claim 1, therefore is rejected for all the same reasons as claim 1 above.

9. With respect to claims 2, 21, 40 and 59, it is rejected for the same reasons as claims 1, 20, 39, and 58 above. In addition, Rakavy discloses a trusted module coupled with the embedded firmware agent and the embedded controller agent, the trusted module to perform cryptographic operations to support operations by the embedded controller agent (col. 9, lines 41-60).

10. With respect to claims 3, 22, 41, and 60, Gibbons discloses the embedded controller agent asserts a management interrupt signal to invoke the management mode (col. 9, lines 45-52, in the background of the application [0003], a system management interrupt is also known as SMI).

11. With respect to claims 4, 23, 42, and 61, it is rejected for the same reasons as claims 1, 20, 39, and 58 above. In addition, Rakavy discloses the embedded controller agent and the embedded firmware agent interact to provide manageability features to the host system (col. 10, lines 54-65).

12. With respect to claims 5, 24, 43, and 62, it is rejected for the same reasons as claims 1, 20, 39, and 58 above. In addition, Rakavy discloses wherein the manageability features are provided prior to the host operating system being loaded (col. 17, lines 8-18, col. 3, lines 16-25, this is done prior to boot strapping).

13. With respect to claims 6, 25, 44, and 63, it is rejected for the same reasons as claims 1, 20, 39, and 58 above. In addition, Rakavy discloses wherein the manageability features are provided after the host operating system has been loaded (col. 11, lines 6-19, this is done while real-mode operating systems are running).

14. With respect to claims 7, 26, 45, and 64, it is rejected for the same reasons as claims 1, 20, 39, and 58 above. In addition, Rakavy discloses the manageability features are provided concurrently with loading of the host operating system (col. 6, lines 60-65).

15. With respect to claims 8, 27, 46, and 65, it is rejected for the same reasons as claims 1, 20, 39, and 58 above. In addition, Rakavy discloses the manageability

features comprise host operating system independent update of a flash memory device via the embedded controller agent (col. 7, lines 19-25, copies the network enhanced bios).

16. With respect to claims 9, 28, 47, and 66, it is rejected for the same reasons as claims 1, 20, 39, and 58 above. In addition, Rakavy discloses the manageability features comprise monitoring of host functionality and reporting to a remote device via the embedded controller agent (col. 9, lines 20-39, col. 15, lines 60-67, col. 16, lines 1-4).

17. With respect to claims 10, 29, 48, and 67, it is rejected for the same reasons as claims 1, 20, 39, and 58 above. In addition, Rakavy discloses the manageability features comprise providing boot services to the host system via the embedded controller agent (col. 10, lines 60-65).

18. With respect to claims 12, 31, 50, and 69, it is rejected for the same reasons as claims 1, 20, 39, and 58 above. In addition, Rakavy discloses the embedded controller agent and the embedded firmware agent interact to provide security features to the host system (col. 9, lines 41-60, security features are enhanced by the bios).

19. With respect to claims 13, 32, 51, and 70, it is rejected for the same reasons as claims 1, 20, 39, and 58 above. In addition, Rakavy discloses the security features are

provided prior to the host operating system being loaded (col. 7, lines 8-18, col. 3, lines 16-25, this is done prior to boot strapping).

20. With respect to claims 14, 33, 52, and 71, it is rejected for the same reasons as claims 1, 20, 39, and 58 above. In addition, Rakavy discloses the security features are provided after the host operating system has been loaded (col. 10, lines 6-19, this is done while real-mode operating systems are running).

21. With respect to claims 15, 34, 53, and 72, it is rejected for the same reasons as claims 1, 20, 39, and 58 above. In addition, Rakavy discloses wherein the security features are provided concurrently with loading of the host operating system (col. 6, lines 60-65).

22. With respect to claims 16, 35, 54, and 73, it is rejected for the same reasons as claims 1, 20, 39, and 58 above. In addition, Rakavy discloses wherein the security features comprise performing verification of the host system (col. 9, lines 45-49) and selectively reporting results to a remote device via the embedded controller agent (col. 9, lines 45-47).

23. With respect to claims 18, 37, 56, and 75, it is rejected for the same reasons as claims 1, 20, 39, and 58 above. In addition, Rakavy discloses wherein the security features comprise providing authentication services for the host system via the

embedded controller agent (col. 9, lines 40-45).

24. With respect to claims 19, 38, 57, and 76, it is rejected for the same reasons as claims 1, 20, 39, and 58 above. In addition, Rakavy discloses wherein the security features comprise providing support for mutual authentication of a network communication session (col. 9, lines 50-59).

25. **Claims 17, 36, 55, and 74 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gibbons in view of Rakavy and in further view of Falik and in even further view of Herzi as applied to claims 1, 12, 20, 31, 39, 50, 58, and 69 and in even further view of Dennis (US Patent # 6,792,556 B1, hereinafter Dennis).**

26. With respect to claims 17, 36, 55, and 74, Gibbons and Rakavy do not disclose wherein the security features comprise performing virus recovery operations via the embedded controller agent.

In the same field of endeavor, Dennis discloses wherein the security features comprise performing virus recovery operations via the embedded controller agent (col. 3, lines 47-59).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the teachings of Gibbons, Rakavy, Falik, and Herzi with the teachings of Dennis in order to restore the boot record if it is a mismatch or if a virus is detected.

Conclusion

27. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 11/24/2008 has been entered.

28. Any inquiry concerning this communication or earlier communications from the examiner should be directed to HO SHIU whose telephone number is (571)270-3810. The examiner can normally be reached on Mon-Thur (8:30am - 4:00pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ario Etienne can be reached on 571-272-4001. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

HTS
01/30/2009

Ho Shiu
Patent Examiner
GAU 2457

/ARIO ETIENNE/

Supervisory Patent Examiner, Art Unit 2457